COPIA OFICIAL
CONVENIO DE PARIS
- LISBOA 1958 -

REPUBLICA ARGENTINA

Ministerio de Economía
y Obras y Servicios Públicos
Instituto Nacional de la Propiedad Industrial

CERTIFICADO DE DEPOSITO

ACTA N° P 02 01 04434

El Comisario de la Administración Nacional de Patentes, certifica que con fecha 19 de NOVIEMBRE de 2002 se presentó a nombre de BELLONI, FABIAN ARMANDO; SCHIAVONI, JUAN JOSE; SCOCHET GABRIEL EDGARDO Y SEMINO DARIO JAVIER; con domicilio en DON BOSCO, PCIA. DE BUENOS AIRES. REPUBLICA ARGENTINA (AR).

una solicitud de Patente de Invención relativa a: "METODO DE PROTECCION DE PROGRAMAS Y EQUIPO PARA REALIZARLO".

cuya descripción y dibujos adjuntos son copia fiel de la documentación depositada en el Instituto Nacional de la Propiedad Industrial.

Se certifica que lo anexado a continuación en fojas CUARENTA es copia fiel de los registros de la Administración Nacional de Patentes de la República Argentina de los documentos de la solicitud de Patentes de Invención precedentemente identificada.

A PEDIDO DEL SOLICITANTE Y DE CONFORMIDAD CON LO ESTABLECIDO EN LA CONVENCION DE PARIS (LISBOA 1958), APROBADO POR LEY 17.011, EXPIDO LA PRESENTE CONSTANCIA DE DEPOSITO EN BUENOS AIRES, REPUBLICA ARGENTINA, A LOS VEINTIUN DIAS DEL MES DE AGOSTO DE 2003.

Ing. LUIS M. NOGUES
COMISARIO
Administración Nacional de Patentes

Memoria Descriptiva

de la Patente de Invención

denominada

"MÉTODO DE PROTECCIÓN DE PROGRAMAS Y EQUIPO PARA REALIZARLO"

Solicitada por: BELLONI, Fabián Armando;
SCHIAVONI, Juan José
SCOCHET, Gabriel Edgardo;
SEMINO, Darío Javier

residentes en: Gral. Roca 1138 (CP 1876) - Don Bosco
Pvcia. de Buenos Aires

Inventores: BELLONI, Fabián Armando
SCHIAVONI, Juan José
SCOCHET, Gabriel Edgardo
SEMINO, Darío Javier

Por el plazo de 20 años

La presente invención se refiere a un método de protección de programas de computación, contra la copia y el uso no autorizado, y el equipo para realizarlo.

El método de protección de programas de la invención se realiza mediante la ejecución de partes seleccionadas del código máquina del programa a proteger (protegido), dentro de un ambiente seguro conformado por un "dispositivo de protección", donde durante la ejecución de dichas partes del código máquina del programa protegido dentro de dicho "dispositivo de protección", la "computadora" (que ejecuta el programa protegido) comparte sus recursos con dicho "dispositivo de protección" de tal manera que pueden ser utilizados por éste último; y donde la computadora está conectada con el mismo a través de uno de sus puertos de comunicación.

Se entiende como recursos de la computadora, a los recursos de equipamiento (hardware) y del sistema operativo que la misma posee.

La invención puede ser aplicada para proteger sistemas de control de procesos, sistemas de control de equipos, programas para telefonía celular, programas para computadoras portátiles, programas para equipos embebidos, programas de computación en general y controladores en general.

El método de protección de programas de la invención incluye:

- Un proceso de extracción de partes del código máquina, que denominaremos "módulos", del programa de computación a proteger.
- El almacenamiento de los módulos obtenidos en un dispositivo de protección que consta como mínimo de un microprocesador, memoria volátil y memoria no volátil.
- Una comunicación entre la computadora y el dispositivo de protección.
- El reemplazo del código máquina de los módulos obtenidos, por llamados a ejecución de dichos módulos dentro del dispositivo de protección.

- La incorporación al programa de computación protegido, de un programa de computación adicional que auspicia de interfaz d comunicación entre la computadora y el dispositivo de protección.
- El procesamiento del programa de computación protegido, entre la computadora y el dispositivo de protección, donde la primera comparte los recursos con el segundo durante la ejecución de las partes del programa protegido dentro del dispositivo de protección.

El proceso de extracción de partes del programa de computación, permite la selección en forma manual o automática de los módulos que serán extraídos, para luego ser almacenados dentro del dispositivo de protección.

El equipo para implementar y ejecutar el método de protección de programas de la invención consta de:

- Una computadora donde se procesa el programa de computación a proteger y se realiza el proceso de extracción de partes del código máquina "módulos" del mismo.
- Un dispositivo de protección que consta como mínimo de un microprocesador, memoria volátil y memoria no volátil donde se almacenan los módulos obtenidos, y donde dicha memoria no puede ser leída desde el exterior.
- Un medio de comunicación entre la computadora y el dispositivo de protección.
- Un programa de computación adicional que auspicia de interfaz de comunicación entre la computadora y el dispositivo de protección.
- Recursos de la computadora compartidos con el dispositivo de protección durante la ejecución de dichos módulos dentro de dicho dispositivo.

Se utiliza como medio de comunicación entre la computadora y el dispositivo de protección, cualquiera de los puertos de comunicación que posee una computadora.

Desde el comienzo de la computación e incrementándose con el aumento en la popularidad de las computadoras personales, la piratería de programas de computación ha sido un problema para sus desarrolladores y fabricantes.

Aunque existen leyes que establecen la ilegalidad de la copia y el uso no autorizado de programas de computación, lo cierto es que igualmente se sigue haciendo uso ilegal de dicha información.

El auge de Internet provocó ventajas y también desventajas, porque si bien Internet es una herramienta poderosa de promoción y venta de productos, también es una herramienta poderosa de distribución de copias piratas o "parches" que eliminan la protección que pudieran tener.

Si bien existen varios métodos de protección contra la copia y el uso no autorizado de programas de computación, ninguno hasta ahora a demostrado ser lo suficientemente eficiente.

Es deseable que los métodos de protección cumplan con algunos requerimientos mínimos para poder ser considerados como tal. Estos requerimientos son:

a) Debe prohibir la ejecución total o parcial no autorizada del programa de computación protegido.

b) Debe brindar protección contra la ingeniería inversa del programa de computación protegido.

c) Debe impedir que la protección pueda ser evadida.

d) Debe poder ser utilizado en una configuración de computadora estándar.

e) Debe permitir la distribución del programa de computación protegido por los canales comunes ya sean Internet, CD-ROM, disco flexible, etc.

f) Debe permitir la actualización del programa de computación protegido.

Con el paso del tiempo surgieron muchos métodos y dispositivos diferentes, y paralelamente surgieron los métodos que los atacan y los vulneran.

Los primeros incorporaban una clave que el usuario debe ingresar para comenzar la ejecución del programa de computación, pero esa clave se difundía rápidamente y el programa de computación quedaba inmediatamente sin protección alguna.

Luego llegaron los dispositivos externos conocidos como "dongles", descriptos por ejemplo en las patentes U.S. Pat. No. 4609777 y U.S. Pat. No. 4685055. Estos dispositivos almacenan las claves que antes ingresaba el usuario, lo que hace imprescindible la existencia del mismo conectado a la computadora para permitir la ejecución del programa de computación. No obstante ésta protección se traduce a un simple salto condicional en el código máquina del programa de computación protegido, que puede ser reemplazado en forma sencilla por un atacante sin demasiada experiencia.

Al aumentar la velocidad de procesamiento de las computadoras, surgieron nuevos métodos conocidos como empaquetado, que incluyen el encriptado del código máquina del programa de computación protegido. Estos métodos tienen el objetivo principal de proteger el código máquina contra la ingeniería inversa. No obstante, debido a que para poder ser ejecutado, el mismo debe ser almacenado en la memoria RAM de la computadora, en ese momento puede obtenerse el código completo desencriptado haciendo un volcado de la memoria RAM a un archivo. Un método similar al mencionado está expuesto en U.S. Pat. No. 5530752.

Al ir aumentando la capacidad de almacenar información y procesamiento de los dispositivos externos (como las "dongles"), podemos encontrar patentes como por ejemplo GB2149944, donde son utilizados para guardar una parte del código del programa de computación protegido que puede o no estar encriptada, o para desencriptar partes d código encriptadas y almacenadas en la computadora. De ésta manera sin

el dispositivo conectado a la computadora no se puede obtener el código completo listo para ser ejecutado, otorgando así protección contra la copia y el uso no autorizado del programa de computación. Sin embargo aunque el código completo del programa de computación protegido no puede obtenerse en su medio de distribución normal, tal como sucede en el método anterior, para que el código sea interpretado por la computadora se debe desencriptar y cargar en la memoria RAM. Es en éste lugar donde el programa de computación queda desprotegido y es finalmente atacado.

Los métodos mencionados anteriormente son muy débiles como mecanismos de protección debido a que no consideran lo pública y de fácil acceso que resulta ser la memoria RAM de la computadora.

Una excepción al problema anterior, son los métodos que almacenan y ejecutan partes del programa de computación protegido dentro de un dispositivo externo a la computadora. De esta forma el programa de computación necesita de la presencia del dispositivo externo para poder ser ejecutado, ofreciendo así protección contra el uso no autorizado. Además un atacante no tiene acceso a dichas partes del programa de computación, quedando imposibilitado de realizar la ingeniería inversa del mismo para evadir la protección.

Dentro de los métodos que incluyen el concepto anterior podemos mencionar los expuestos en las patentes EP0266748 o U.S. Pat. No. 4817140, GB2122777, U.S. Pat. No. 4634807 o GB2163577, U.S. Pat. No. 5754646, U.S. Pat. No. 6266416 y U.S. Patent Application. No. 20010056539. Estos métodos de protección utilizan un dispositivo externo conectado a la computadora que está ejecutando el programa de computación protegido. En dicho dispositivo, algunos métodos ejecutan parte del código protegido que se encuentra dentro del mismo y otros desencriptan y ejecutan dentro de dicho dispositivo partes del código protegido. Para ofrecer mas seguridad durante la comunicación, algunos métodos encriptan la información intercambiada entre la computadora y el dispositivo externo.

En todos los casos mencionados, puede asociarse al dispositivo externo con una caja negra a la cual se les pasan parámetros y se obtienen resultados como respuesta.

En estos métodos, el dispositivo externo ejecuta una subrutina que está imposibilitada de acceder a una subrutina o variable externa. Esta subrutina debe seleccionarse de tal manera que obteniendo los parámetros y resultados no pueda ser inferida.

En forma aparente, estos métodos ofrecen total protección, porque cumplen con la premisa de que la verdadera forma de proteger programa de computación es ejecutando partes del programa de computación protegido en un ambiente seguro fuera de la computadora, evitando la posibilidad de ser analizados con ingeniería inversa. No obstante no tienen en cuenta algo muy importante, si bien el atacante (persona interesada en vulnerar, copiar o usar en forma no autorizado el programa) no sabe lo que se está ejecutando dentro del dispositivo, y suponiendo que el código dentro del dispositivo no puede ser deducido, puede almacenar los parámetros y sus correspondientes resultados, y luego realizar una tabla que termina reemplazando al dispositivo externo.

El hecho de que la memoria de la computadora no pueda ser accedida por el código que se está ejecutando dentro de la computadora o que no se puedan hacer llamados a subrutinas o funciones externas, disminuye el grado de protección que pueden brindar.

Existen métodos que también ejecutan parte del programa de computación protegido en un dispositivo externo u otra computadora, pero en una arquitectura en red como los revelados en las patentes U.S. Pat. No. 6009543 y U.S. Pat. No. 6343280. A diferencia de los anteriores, el método de la patente U.S. Pat. No. 6343280 agrega la copia de la memoria RAM de la computadora. En éste último, un cliente que está ejecutando el programa de computación protegido debe presentar una clave de acceso a un dispositivo denominado "License S rver" alojado en l servidor, que ejecutará parte del programa de computación protegido cuando así se lo

requiera la aplicación ejecutada en el cliente. El "License Server" puede ser interpretado como una caja negra que recibe parámetros y devuelve resultados los cuales incluyen la copia de la memoria de la computadora. De ésta manera la cantidad de parámetros y resultados aumentan considerablemente con respecto a los métodos mencionados anteriormente. Al igual que en los métodos anteriores, el "License Server" no puede hacer llamados a subrutinas o funciones externas mientras está ejecutando parte del programa de computación protegido.

Si bien la mayor cantidad de parámetros y resultados hace más difícil la construcción de una tabla, ésta puede ser construida igualmente para atacarlo.

Sin embargo existen tres puntos que hacen que éste método sea inviable como método de protección con dispositivo externo.

Primero, considerando que una aplicación puede direccionar hasta 4Gb de memoria RAM, es necesario que el "License Server" pueda tener ésta capacidad de memoria o cómo mínimo la misma capacidad de memoria que tiene la computadora del cliente donde se está ejecutando el programa de computación protegido, para poder hacer la copia de memoria. Esto obliga a que el "License Server" deba ser implementado en un dispositivo más costoso que uno que utilice un microcontrolador porque su memoria RAM es muy inferior a 4Gb. De la misma manera en el futuro, a medida que aumenten las capacidades de memoria de las computadoras, tendrá que aumentar la capacidad de memoria del "License Server".

Segundo, el método termina no siendo un verdadero método de protección. Esto es porque la única protección que tiene frente a varios clientes que quieran usar el programa de computación protegido, es la presentación de la clave de acceso al "License Server" para que comience su ejecución. Teniendo en cuenta esto último, un atacante puede conseguir en forma sencilla una clave de acceso adquiriendo así autorización al uso del programa de computación protegido.

Tercero, debido a que la cantidad de usuarios que pueden ejecutar el programa de computación protegido (cantidad de licencias) al mismo tiempo está limitada por la dirección de IP, puede utilizarse un PROXY o RUTEADOR conectado a la red que contiene el "License Server", permitiendo acceder con la misma IP a indefinida cantidad de usuarios extras.

La presente invención, no solo mejora y supera a los métodos descriptos anteriormente, sino que hace que la ingeniería inversa del programa de computación protegido resulte inviable, protegiéndolo finalmente contra la piratería.

La novedad de la presente invención consta en un método en el cual partes de código máquina del programa de computación a proteger, o "módulos", son extraídos y almacenados dentro de la memoria de un "dispositivo de protección". Dichos módulos son reemplazados en el programa de computación protegido por llamados a ejecución de dichos módulos dentro del dispositivo de protección y código basura. Dicha memoria del dispositivo de protección que contiene los módulos, no puede ser leída desde el exterior, y donde durante la ejecución de dichas partes del código máquina del programa protegido dentro de dicho "dispositivo de protección", la computadora (que ejecuta el programa protegido) comparte sus recursos con dicho "dispositivo de protección".

Para mayor aclaración se indica que se llama código máquina, al lenguaje de mas bajo nivel de la computadora, que representa instrucciones y datos de un programa ejecutable por la misma.

El método de protección de programas de computación, de la presente invención, consta de las siguientes etapas:

(a) - Extracción d módulos: Extraer de la computadora una o más partes de código máquina del programa de computación a proteger, llamados "módulos", previamente seleccionados, de forma tal que el código máquina que poseen contenga al menos instrucciones que

interrumpen y direccionen el curso de ejecución del programa, instrucciones que accedan a variables externas e instrucciones que agrupadas ofrecen muy alta dificultad de ser inferidas.

(b) - Almacenamiento de los módulos: Almacenar dichos "módulos" dentro de la memoria de un "dispositivo de protección", que no puede ser leída desde el exterior.

(c) - Reemplazo de los módulos: Reemplazar dichos "módulos" en el programa de computación protegido por llamados a ejecución de esos módulos dentro del dispositivo de protección.

(d) - Comienzo de la ejecución de la parte pública del programa: Luego de implementada la protección según las etapas anteriores, se comienza la ejecución de la parte pública del programa que contiene los llamados a ejecución de cada módulo.

(e) - Ejecución de módulos: Donde durante la ejecución de esos módulos dentro del dispositivo de protección se utilizan los recursos de la computadora pudiendo remitir al acceso de la memoria, o a la ejecución de funciones o subrutinas dentro de la misma. Eventualmente la ejecución de esos módulos dentro del dispositivo externo de protección, puede remitir a la ejecución de funciones o subrutinas que se encuentran en otros módulos dentro del mismo dispositivo.

(f) - Retorno a la computadora: Retornar el hilo de ejecución a la computadora una vez ejecutado el módulo.

De ésta manera se obtiene una parte pública del programa de computación protegido que se almacena y ejecuta dentro de la computadora, y una parte privada del mismo que se almacena y ejecuta dentro del dispositivo de protección.

Los módulos extraídos no necesariamente deben ser funciones o subrutinas a las cuales se les pasa parámetros y se obtienen resultados.

Esto se logra gracias a que el dispositivo de protección, realiza el procesamiento compartido del programa de computación protegido junto con el procesador de la computadora, emulándolo. De ésta manera, el programa de computación podrá ejecutarse parcial o totalmente sólo si existe el dispositivo de protección.

Para poder llevar a cabo la ejecución del programa de computación protegido entre la computadora y el dispositivo de protección, la memoria de la computadora y sus registros internos son compartidos con el dispositivo de protección. Esto hace que el dispositivo externo no sea sólo una caja negra con una entrada y una salida, sino que está provista por indefinidas entradas y salidas que interactúan directamente con los recursos de la computadora durante la ejecución del programa de computación protegido. A esto se le suma el hecho de que, tal como sucede en un sistema realimentado, las salidas pueden volver a utilizarse como entradas.

El llamado a funciones o subrutinas no se limita a que se lleven a cabo sólo en la computadora, sino que durante la ejecución del programa de computación dentro del dispositivo de protección pueden existir llamados a funciones o subrutinas externas, continuando a su retorno, con la ejecución dentro del mismo. También pueden existir llamados a funciones internas que pueden o no estar en otro módulo dentro del mismo dispositivo de protección. Además, puede existir un llamado a ejecución no sólo a partir del comienzo de un módulo determinado, sino que a cualquier parte del mismo.

Como resultado final el atacante, no solo queda imposibilitado de ver o inferir el código almacenado y ejecutado en el dispositivo de protección, sino que además al existir indefinidas entradas y salidas de datos del dispositivo de protección, y por ende prácticamente infinitas relaciones parámetros/resultado que además pueden estar relacionadas entre sí, la construcción de una tabla es inviable. Por esto último, el encriptado d la comunicación se hace innecesario. Aunque la comunicación sea

encriptada, para ser interpretada hay que desencriptar y es finalmente en éste lugar donde se hacen vulnerables los mecanismos que basan su protección en el encriptado.

Debido a que cada dispositivo de protección y cada programa protegido poseen un identificador único e irrepetible que permiten identificarse entre si, podrán ejecutarse varios programas protegidos con la presente invención al mismo tiempo, siempre y cuando su dispositivo de protección correspondiente esté presente y conectado al puerto de la computadora.

El método de protección de programas de computación, contra la copia y el uso no autorizado, de la invención, brinda una habilitación al uso del programa protegido, que puede estar limitada a un tiempo de uso previamente establecido.

El objetivo principal del método de protección de programas de computación, de la invención, es evitar la copia e impedir el uso no autorizado total o parcial del mismo; brindar protección contra la ingeniería inversa del programa de computación protegido e impedir que la protección pueda ser evadida.

Un segundo objetivo del método de protección de programas de la presente invención es desarrollar una secuencia tal que sea imposible la construcción de una tabla de datos para atacar al método y vulnerar la protección del programa.

Un tercer objetivo del método de protección de programas de la presente invención es proteger, de la misma forma, al programa de computación que utiliza el concepto de licencias, utilizado cuando un usuario del programa de computación protegido adquiere varios programas para ser utilizados en red. En este caso el dispositivo de protección puede ser instalado en una computadora perteneciente a dicha red.

Un objetivo adicional de la invención es obtener un equipo para desarrollar el método de protección de programas de la presente invención.

Algunas aplicaciones de la invención son la protección de: sistemas de control de procesos, sistemas de control de equipos y programas para telefonía celular.

Otras aplicaciones de la invención son la protección de programas para computadoras portátiles, programas para equipos embebidos y programas de computación en general.

El método de protección de programas de computación, de la invención, puede ser de mejor entendimiento a través de una descripción detallada de la totalidad de su realización, que será ampliada más adelante al describir las figuras, en especial la Figura 6. A tal fin se puede dividir en 2 partes.

La primera parte es en la cual se implementa el mecanismo de protección en el programa a proteger, generalmente realizada por su fabricante. La segunda, realizada, durante la ejecución del programa protegido en la computadora del usuario final del mismo.

PARTE 1

1.- Una vez finalizado y obtenido el o los archivos ejecutables del programa de computación a proteger, se extraen del o los mismos, partes de código máquina "módulos" previamente seleccionados, de forma tal que el código máquina que poseen contenga al menos instrucciones que interrumpen y direccionen el curso de ejecución del programa, instrucciones que accedan a variables externas e instrucciones que agrupadas ofrecen muy alta dificultad de ser inferidas.

La extracción de éstos módulos puede realizarse en forma automática o manual. (Etapa a)

2.- Los módulos extraídos son identificados individualmente, almacenados en el dispositivo de protección y reemplazados en el programa por un salto a ejecución del módulo correspondiente dentro del dispositivo de protección y por código basura de relleno. (Etapas b y c)

3.- Se obtienen una parte pública del programa protegido que se instalará y ejecutará en la computadora del usuario final del programa protegido, y una parte privada que se encuentra dentro del dispositivo de protección. De tal manera que el usuario del programa protegido, sólo lo podrá ejecutar totalmente si posee el dispositivo de protección correspondiente conectado en uno de los puertos de la computadora. La habilitación al uso del programa protegido, que puede estar limitada a un tiempo de uso previamente establecido.

PARTE 2

1.- Comienza con la ejecución de la parte pública del programa protegido en la computadora del usuario (Etapa d). Esta busca si está conectado el dispositivo de protección a la misma, lo identifica y prosigue con la ejecución. En el caso de que el dispositivo de protección no esté conectado o no sea el correspondiente, prosigue o no con la ejecución dependiendo de si se hizo una protección de ejecución total o parcial del programa.

2.- Cuando se encuentra con un salto a ejecución de un módulo que se encuentra dentro del dispositivo de protección, la computadora le pasa el hilo de ejecución a éste último.

3.- Comienza la ejecución de los módulos dentro del dispositivo de protección (etapa e). Para ello el dispositivo de protección recibe de la computadora todos los registros de su procesador, un valor de desplazamiento "offset" de la dirección de inicio de ejecución del módulo y el identificador del módulo a ejecutar.

4.- El dispositivo de protección obtiene del módulo (que se encuentra almacenado en su memoria y no puede ser leído desde el exterior), el código máquina a ejecutar, e interpreta el código de operación de la instrucción.

5.- Analiza si la instrucción interrumpe y direcciona el curso de ejecución del programa (instrucción del tipo CALL, JMP o Jcc) y la ejecuta de ser así.

Analiza si la instrucción a ejecutar contiene un operador que se encuentra en la memoria de la computadora o en la memoria interna y lo obtiene de ser así.

6.- Ejecuta la instrucción emulando al procesador de la computadora.

7.- Analiza si el resultado de la ejecución debe ser almacenado en la memoria de la computadora o en la memoria interna y lo almacena de ser así.

8.- Vuelve a obtener código máquina del módulo que está siendo ejecutado y continúa la ejecución dentro del dispositivo de protección hasta la finalización del módulo o la presencia de una instrucción que interrumpa y direccione la ejecución del programa a la computadora.

9.- El dispositivo de protección retorna el hilo de ejecución a la computadora enviándole a la misma la actualización de todos los registros de su procesador. (etapa f)

10.- Continúa la ejecución de la parte pública del programa protegido en la computadora hasta encontrar un nuevo salto a ejecución de uno de los módulos dentro del dispositivo de protección.

A fin de una mejor comprensión de la presente invención y mayor entendimiento de las ventajas comentadas, más las que los entendidos en la especialidad podrán agregar, se realiza a continuación la descripción detallada del método de protección de programas de computación de la presente invención y del equipo para realizarlo de la presente invención, en base a los dibujos adjuntos, en los cuales:

La figura N 1 muestra la configuración del dispositivo requerida por la presente invención.

La figura N 2 muestra esquemáticamente el funcionamiento del método de protección de programas de computación de la presente invención.

La figura Nº 3 ilustra el proceso de extracción de partes del código máquina del programa de computación a proteger, "módulos".

La figuras Nº 3b y N° 3c ilustran esquemáticamente la carga de módulos dentro del dispositivo de protección.

La figura Nº 4 ilustra la comunicación entre la computadora y el "dispositivo de protección".

La figura Nº 5 muestra el esquema de la ejecución del programa de computación protegido por la presente invención.

La figura Nº 6 muestra el diagrama del proceso de ejecución del "módulo" del método de la presente invención, dentro del dispositivo de protección.

En las figuras, a iguales números de referencia corresponden iguales o equivalentes elementos constitutivos del ejemplo de realización del equipo de la invención y de su instalación.

En la figura Nº 1 se observa la configuración del dispositivo requerida por la presente invención, contiene una computadora personal o estación de trabajo [1] , que contiene instalada la parte pública del programa de computación protegido [2], y un dispositivo externo "dispositivo de protección" [3] conectado a uno de los puertos de comunicación de dicha computadora.

Muestra además que la parte pública del programa de computación protegido puede ser distribuida para la venta a través de una red LAN, WAN o generalmente la más usada Internet [4], o a través de algún medio de almacenamiento de información pudiendo ser óptico, magnético, etc [5].

La distribución de la parte pública del programa de computación protegido a través de Internet implica directamente una libre distribución y

copia de la misma. Sin embargo, debido que la parte privada del programa de computación protegido reside dentro del dispositivo de protección, no se puede obtener una copia total del programa de computación protegido.

Además, debido a que la ejecución en forma parcial o total del programa de computación protegido requiere del dispositivo de protección, queda restringido su uso no autorizado.

En la figura Nº 2 se observa esquemáticamente el funcionamiento del programa de computación protegido por la presente invención. El programa de computación a proteger [6], que llamaremos "App.exe", está dividido en dos partes: una parte pública, compuesta por partes del programa [7] [8] [9] y [10], y una parte privada, compuesta por otras partes, denominados "módulos" [11] [12] y [13].

Dicha figura 2 permite observar que las partes privadas, módulo 1 [11], módulo 2 [12], módulo n [13] del programa de computación a proteger [6], son extraídos y almacenados dentro del dispositivo de protección [3]. Las partes restantes del programa de computación a proteger [7] [8] [9] y [10] forman la parte pública del programa de computación protegido [2], que llamaremos "APP.exe_pc" ("APP.exe" sin los módulos 1,2,...n), son almacenadas en la computadora [1] donde luego se ejecutará el programa de computación protegido. La unión de los módulos que contiene el dispositivo de protección " Módulo 1 + Módulo2 + ... + Módulo n" y las partes restantes "APP.exe_pc" que contiene la computadora, hacen que se obtenga nuevamente "APP.exe" [14].

Podemos inferir entonces que sin el dispositivo de protección, el programa de computación protegido no se podrá ejecutar o se podrá ejecutar solo parcialmente dependiendo de las partes extraídas del programa de computación sin proteger.

La ejecución parcial del programa de computación protegido puede ser de utilidad para obtener versiones de evaluación del mismo. Estas

versiones, son muy usadas actualmente como formas de promoción y comercialización. De esta manera el programa de computación protegido permite la opción "pruebe y luego compre", ya que no podrá utilizarse en su totalidad sin la presencia del dispositivo de protección, la cual debe ser solicitada al fabricante del programa de computación o a su distribuidor.

En la figura Nº 3 se observa el proceso de extracción de las partes del código máquina del programa de computación a proteger o "módulos". El proceso de extracción se lleva a cabo una vez que el programa de computación a proteger está totalmente finalizado, ya que el método de protección de la presente invención, no se implementa durante el desarrollo del mismo y no requiere del uso de APIs (se llama así a la Interfaz de Programación de Aplicaciones, conjunto de rutinas, protocolos, y herramientas para construir programas de computación)

Está compuesto por las siguientes operaciones:

a) Selección de los módulos [11] [12] [13] en forma manual o automática:

- La selección de los módulos [11] [12] [13] en forma manual, permite que el fabricante del programa de computación a proteger [6], seleccione las partes del mismo que se ejecutarán sólo si el dispositivo de protección se encuentra presente. De ésta forma se pueden obtener versiones de evaluación o versiones que según el dispositivo de protección puedan ejecutar total o parcialmente la aplicación. El módulo seleccionado no necesariamente debe ser una función o subrutina, y puede hacer uso de cualquier variable alocada en la memoria de la computadora y contener llamados a funciones externas.
- La selección de los módulos [11] [12] [13] en forma automática facilita al fabricante del programa de computación la implementación de la protección, y hace que el programa de computación protegido no pueda ser ejecutado sin la presencia del dispositivo de protección.

b) Extracción de los módulos seleccionados [15] para luego ser almacenados dentro del dispositivo de protección.

c) Carga de los módulos seleccionados en el dispositivo de protección: Los módulos extraídos [11] [12] [13] del programa de computación a proteger [6], son cargados en el dispositivo de protección [3], luego de presentar correctamente una clave [19] que habilita la carga de dichos módulos, obteniéndose los correspondientes módulos [16] [17] [18] en dicho dispositivo de protección [3]. La presentación de dicha clave tiene un máximo de 3 reintentos inválidos, de esta manera se evita la fuerza bruta como mecanismo para obtener la clave ilegalmente. Cada módulo que se carga en el dispositivo de protección tiene un número que lo identifica y lo individualiza de los demás.

La operación de carga puede contener un proceso de encriptado de cada módulo antes de ser cargado en el dispositivo de protección, para que luego ésta última lo desencripte y lo almacene desencriptado dentro de sí misma. (ver Fig. 3b)

d) El reemplazo de los módulos seleccionados por llamados a ejecución [20] [21] [22] de dichos módulos [16] [17] [18], que ahora se encuentran dentro del dispositivo de protección.
En los lugares del programa de computación sin proteger [6] "APP.exe" donde se extrajo cada uno de los módulos, se introduce código de relleno y un llamado a ejecución del módulo correspondiente [20] [21] [22] para que se ejecute dentro de el dispositivo de protección [3]. (ver Fig. 5)

e) Incorporación en el código máquina de la parte pública del programa de computación protegido, de un programa de computación adicional [23] que hace de "Interfaz" de comunicación entre la computadora y el dispositivo de protección.

Al código máquina del programa de computación original [6] "APP.exe" sin las partes extraídas [11] [12] [13] "módulos" y con el

programa de computación adicional [23], lo llamamos "APP.exe_pc" y es la parte pública del programa de computación protegido [24] que se encuentra en la computadora (equivalente al identificado como [2]).

En la figura Nº 3b se observa esquemáticamente la carga de módulos dentro del dispositivo de protección: La operación de carga puede contener un proceso de encriptado y desencriptado de cada módulo. De ésta manera, se lo provee al usuario de la presente invención, de un método seguro de actualización del programa de computación protegido. Se realiza a continuación la descripción de las 2 variantes, es decir con el encriptado o sin él.

Supongamos que una empresa desarrolladora de programa de computación saca al mercado su producto protegido con la presente invención; y luego de unos meses descubre que el programa de computación protegido tiene un problema en una parte del código que casualmente se encuentra dentro del dispositivo de protección. La empresa puede reemplazar dicho módulo utilizando dos métodos posibles: el primero es reemplazando el dispositivo de protección, y el segundo es reemplazando solamente el módulo con la falla.

Esta última acción tiene el inconveniente de que para reemplazar dicho módulo, la empresa debe hacer público el código máquina del mismo, ya que deberá entregárselo a cada usuario del programa de computación protegido para que finalmente éste último lo cargue dentro del dispositivo de protección.

Utilizando la operación de carga encriptada y entregando el módulo que debe ser reemplazado dentro del dispositivo ya encriptado, la empresa se asegura que el mismo no podrá ser utilizado para quebrar la protección.

Los módulos extraídos [25] del programa de computación sin proteger son encriptados por una unidad de encriptado [26], cuya clave

de desencriptado [27] se encuentra almacenada dentro del dispositivo de protección.

Los módulos encriptados [28] son desencriptados por la unidad de desencriptado [29] que se encuentra dentro del dispositivo de protección [3], y almacenados dentro del mismo.

En la figura Nº 3c se observa esquemáticamente la carga de módulos dentro del dispositivo de protección: sin el proceso de encriptado mencionado, es decir la segunda variante.

Durante la etapa de producción, las empresas fabricantes del programa de computación protegido, pueden utilizar la operación de carga sin encriptado [30] como se detalló anteriormente, ya que dicho proceso se lleva a cabo dentro de la misma empresa sin necesidad de hacer público el código máquina de cada módulo.

En la figura Nº 4 se observa la comunicación entre la computadora [1] y el dispositivo de protección [3]. En el mismo diagrama se puede observar la configuración mínima de dispositivo que constituye el dispositivo de protección: microprocesador [31], memoria ROM o Flash EPROM [32], memoria EEPROM [33], memoria RAM [34], puerto de comunicación [35] y puede o no contener un coprocesador criptográfico [36].

Durante la ejecución del programa de computación protegido, el sistema operativo de la computadora carga la parte pública del programa de computación protegido [24], "APP.exe_pc" en memoria [37] para ser ejecutado. Cuando "APP.exe_pc" requiere ejecutar parte del código que se encuentra dentro del dispositivo de protección [3], utiliza la INTERFAZ [23] para enviar a través del puerto de comunicación [39] el comando respectivo al dispositivo.

Por medio de la misma INTERFAZ [23], y del puerto de comunicación [35] el dispositivo de protección [3] accede a subrutinas, registros y memoria de la computadora, y una vez finalizada la ejecución del módulo, retorna el control de ejecución del programa de computación protegido, al procesador de la computadora [40] y a la parte pública del programa de computación protegido [24] "APP.exe_pc" .

En la figura Nº 5 se observa el esquema de la ejecución del programa de computación protegido por la presente invención.

Comienza en la computadora [1] con la ejecución de la parte pública del programa de computación protegido [24] "APP.exe_pc". y sigue dentro de la misma hasta que encuentra un llamado a ejecución [20] [21] [22] de uno de los módulos [16] [17] [18] dentro del dispositivo de protección [3]. En ese momento se le transfieren a éste último los registros del procesador [41] y también se le transfiere el hilo de ejecución a través de la interfaz [23] y de los puertos de comunicación [39] y [35].

Durante la ejecución del módulo [16] [17] [18], el dispositivo de protección [3] puede acceder a la memoria de la computadora [37] para extraer o almacenar información si así se requiere o puede hacer saltos a funciones o subrutinas [43] que se encuentran dentro de la computadora para luego del retorno [44] continuar con la ejecución. Cada vez que encuentre un salto a subrutina [43], el dispositivo [3] debe enviarle a la computadora [1] los registros del procesador [41] tal como el los haya modificado anteriormente [42]. De esta forma la ejecución de la subrutina dentro de la computadora se lleva a cabo correctamente y luego retorna la ejecución al dispositivo de protección.

Una vez finalizada la ejecución del módulo [16] [17] [18], el dispositivo de protección retorna el hilo de ejecución a la computadora retornándole los registros del procesador modificados o no dependiendo del código máquina ejecutado.

Para mayor aclaración de la presente invención, y la manera que la misma ha de ser llevada a la práctica, se explican a continuación **un ejemplo de realización de la invención**:

Se aplicó el método de protección de la invención a un programa de control de bordado de telas, utilizando el proceso de extracción de los módulos descripto en las figuras anteriores.

Conectado al puerto USB de la computadora que controla la máquina de bordado, se utilizó un dispositivo de protección al cual se le introdujo los módulos extraídos del programa a proteger. De ésta forma, tal como se explicó anteriormente, se obtuvieron dos partes del programa protegido: la primer parte denominada "Parte Pública del Programa Protegido" que se ejecutó en la computadora mencionada anteriormente y una segunda parte denominada "Parte Privada del Programa Protegido" conformada por los módulos extraídos que se ejecutaron en el dispositivo de protección.

En la figura Nº 6 se observa el esquema de realización del método de la invención, en el ejemplo de realización mencionado, y del proceso de ejecución de un "módulo" dentro del dispositivo de protección:

Cuando la ejecución en la computadora del programa de computación protegido encuentra un llamado a ejecución de uno de los módulos, el programa de computación adicional o interfaz [23] (ver Figura 3) le pasa el hilo de ejecución al dispositivo de protección.

Este último recibe de la computadora, a través de la interfaz y de los puertos de comunicación [39] y [35] (ver Figura 4), los registros del procesador, un desplazamiento denominado "offset" que indica a partir de que dirección dentro del módulo debe iniciar la ejecución y el identificador del módulo a ejecutar [45].

El dispositivo de protección, lee el código máquina a ejecutar almacenado como módulo, e interpreta el código de operación para determinar la instrucción que debe emular [46].

Si el código de operación identifica a una instrucción CALL [47] debe determinarse si se hace un llamado a una función o subrutina interna o externa al dispositivo de protección.

Si es una función o subrutina externa [48], el dispositivo de protección envía a la computadora los nuevos valores de los registros y le pasa el hilo de ejecución a la computadora quedándose a la espera del retorno [49]. La computadora ejecuta la función o subrutina solicitada y luego retorna el hilo de ejecución nuevamente al dispositivo de protección. Esta última recibe todos los registros del procesador [50] y continúa con la ejecución del módulo [53].

Si es una función o subrutina interna [51], el dispositivo de protección ejecuta el llamado de la función o subrutina a la dirección especificada por la instrucción CALL, emula el código de la función [52] y retorna nuevamente continuando con la ejecución del módulo [53].

Si el código de operación identifica a una instrucción JMP ya s a condicional o no [54], debe determinarse si se hace un salto a una dirección interna o externa al dispositivo de protección.

Si es un salto a una dirección externa [55], el dispositivo de protección envía a la computadora los nuevos valores de los registros [56], finaliza la ejecución de módulo y le pasa el hilo de ejecución a la computadora [57].

Si el salto es a una dirección interna [58], lo lleva a cabo, y luego continúa con la ejecución del módulo [53].

Si en la instrucción a ser emulada, alguno de los operadores hace referencia a la memoria de la computadora, se determina si es a la memoria interna del dispositivo de protección [63] o a la memoria de la computadora [59]. Si es a la memoria de la computadora el dispositivo d protección accede a la misma a través de la interfaz de comunicación, obtiene el dato requerido y prosigue con la emulación de la instrucción solicitada [60]. En caso de que los operadores no hagan referencia a memoria, continúa con la emulación de la instrucción solicitada [60].

Al finalizar la emulación de la instrucción, si el resultado debe ser almacenado en la memoria de la computadora [61] o en la memoria

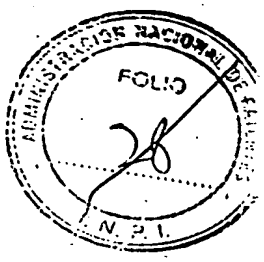
interna [64], el dispositivo de protección accede a la memoria y luego continúa con la ejecución del módulo [53].

Al llegar al final del módulo, el dispositivo de protección envía a la computadora los nuevos valores de lo registros [56], finaliza la ejecución de módulo y le pasa el hilo de ejecución a la computadora [57] quedando en espera a un nuevo pedido de ejecución de uno de los módulos.

En caso contrario [62], lee el siguiente código máquina a ejecutar, e interpreta el código de operación [46] para continuar con la ejecución del módulo.

De la experiencia realizada, podemos concluir diciendo que la ejecución del programa protegido se llevó a cabo en forma compartida entre la computadora y el dispositivo de protección, donde se compartieron los recursos de está última durante la ejecución de los módulos dentro del dispositivo de protección.

Siguen 32 reivindicaciones en página 26.



REIVINDICACIONES

Habiendo descripto y determinado la naturaleza y alcance de la presente invención, y la manera que la misma ha de ser llevada a la práctica, se declara lo que se reivindica como invención y de propiedad exclusiva:

1. Método de protección de programas de computación, contra la copia y el uso no autorizado, que contienen una parte pública del programa protegido de computación, o control, que se carga en memoria y se ejecuta en el procesador (dentro de la computadora), y una parte privada del mismo, caracterizado por comprender, por lo menos, las siguientes etapas:
   (a) - **Extracción de módulos:** extraer del programa de computación a proteger una o más partes de código máquina, llamados "módulos", que constituyen dicha parte privada del programa de computación protegido.
   (b) - **Almacenamiento de los módulos:** almacenar dichos uno o más módulos dentro de la memoria de un dispositivo de protección.
   (c) - **Reemplazo de los módulos:** reemplazar dichos uno o más módulos en el programa de computación protegido por llamados a ejecución de esos módulos.
   (d) - **Comienzo de la ejecución de la parte pública del programa:** luego de implementada la protección según las etapas anteriores, comenzar la ejecución de la parte pública del programa que contiene los llamados a ejecución de cada módulo.
   (e) - **Ejecución de módulos:** ejecutar esos módulos en el dispositivo de protección.
   (f) - **Retorno a la computadora:** retornar el hilo de ejecución a la computadora una vez ejecutado dichos uno o más módulos.
2. Método de protección de programas, según la reivindicación 1, caracterizado porque en dicha etapa (e) de "Ejecución de módulos", se

realiza el procesamiento compartido del programa de computación protegido entre el dispositivo externo de protección y el procesador de la computadora.

3. Método de protección de programas, según la reivindicación 2, caracterizado porque en dicha etapa (e) de "Ejecución de módulos", en la ejecución de los módulos se remite a la ejecución de funciones o subrutinas que se encuentran en otros módulos en el dispositivo de protección y en la computadora, indistintamente.

4. Método de protección de programas, según la reivindicación 2, caracterizado porque en dicha etapa (e) de "Ejecución de módulos", en la ejecución de los módulos se remite a la ejecución de funciones o subrutinas que se encuentran en otros módulos dentro del dispositivo de protección.

5. Método de protección de programas, según la reivindicación 2, caracterizado porque en dicha etapa (e) de "Ejecución de módulos", en la ejecución de cada módulo se remite a la ejecución de funciones o subrutinas que se encuentran en la computadora.

6. Método de protección de programas de computación, contra la copia y el uso no autorizado, según cualquiera de las reivindicaciones anteriores, caracterizado porque en dicha etapa (e) de Ejecución de módulos, el dispositivo de protección accede a la memoria de la computadora para extraer o almacenar información.

7. Método de protección de programas de computación, contra la copia y el uso no autorizado, según la reivindicación 6, caracterizado porque previo a dicha etapa (a) de . Extracción de módulos se realiza una selección de los módulos en forma manual, de forma tal que el código máquina que poseen contenga al menos instrucciones que interrumpen y direccionen el curso de ejecución del programa, instrucciones que accedan a variables externas e instrucciones que agrupadas ofrecen

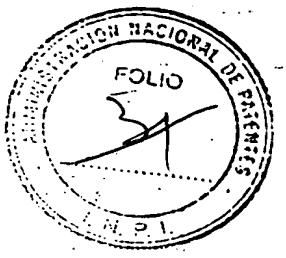
muy alta dificultad de ser inferidas.

8. Método de protección de programas de computación, contra la copia y el uso no autorizado, según la reivindicación 6, caracterizado porque previo a dicha etapa (a) de Extracción de módulos se realiza una selección de los módulos en forma automática, de forma tal que el código máquina que poseen contenga al menos instrucciones que interrumpen y direccionen el curso de ejecución del programa, instrucciones que accedan a variables externas e instrucciones que agrupadas ofrecen muy alta dificultad de ser inferidas.

9. Método de protección de programas de computación, contra la copia y el uso no autorizado, según cualquiera de las reivindicaciones anteriores, caracterizado porque en dicha etapa (b) de Almacenamiento de los módulos, dichos uno o más módulos, son encriptados previamente y desencriptados por el dispositivo de protección durante el almacenamiento, dentro de sí mismo.

10. Método de protección de programas de computación, contra la copia y el uso no autorizado, según cualquiera de las reivindicaciones anteriores, caracterizado porque previo a dicha etapa (e) de Ejecución de módulos en el dispositivo de protección, se realiza la incorporación de un programa de computación adicional en el código máquina de la parte pública del programa de computación protegido, que auspicia de "Interfaz" de comunicación entre la computadora y el dispositivo de protección.

11. Método de protección de programas de computación, contra la copia y el uso no autorizado, según cualquiera de las reivindicaciones anteriores, caracterizado porque la habilitación al uso del programa protegido puede estar limitada a un tiempo de uso previamente establecido.



12. Método de protección de programas de computación, contra la copia y el uso no autorizado, según cualquiera de las reivindicaciones anteriores, caracterizado porque en dicha etapa (e) de Ejecución de módulos dentro del dispositivo externo de protección, el dispositivo de protección recibe los siguientes datos de la computadora, todos los registros de su procesador, un valor de desplazamiento "offset" de la dirección de inicio de ejecución del módulo y el identificador del módulo a ejecutar.

13. Método de protección de programas de computación, contra la copia y el uso no autorizado, según la reivindicación 12, caracterizado porque en dicha etapa (e) de Ejecución de módulos, luego de recibir dichos datos de la computadora, el dispositivo de protección obtiene el módulo que se encuentra almacenado en su memoria, el código máquina a ejecutar, e interpreta el código de operación de la instrucción.

14. Método de protección de programas de computación, contra la copia y el uso no autorizado, según la reivindicación 13, caracterizado porque en dicha etapa (e) de Ejecución de módulos, luego de obtener el módulo, el dispositivo de protección analiza si la instrucción interrumpe y direcciona el curso de ejecución del programa (instrucción del tipo CALL, JMP o Jcc) y la ejecuta de ser así.

15. Método de protección de programas de computación, según la reivindicación 13, caracterizado porque en dicha etapa (e) de Ejecución de módulos, luego de obtener del módulo, el dispositivo de protección analiza si la instrucción a ejecutar contiene un operador que se encuentra en la memoria de la computadora o en la memoria del dispositivo de protección y lo obtiene de ser así.

16. Método de protección de programas de computación, contra la copia y el uso no autorizado, según la reivindicación 13, caracterizado porque en dicha etapa (e) de Ejecución de módulos, el dispositivo de

protección ejecuta la instrucción recibida emulando al procesador de la computadora.

17. Método de protección de programas de computación, contra la copia y el uso no autorizado, según la reivindicación 13, caracterizado porque en dicha etapa (e) de Ejecución de módulos, el dispositivo de protección ejecuta la instrucción recibida emulando cualquiera de las máquinas virtuales JAVA o .NET.

18. Método de protección de programas de computación, contra la copia y el uso no autorizado, según cualquiera de las reivindicaciones 16 y 17, caracterizado porque en dicha etapa (e) de Ejecución de módulos, luego de ejecutar la instrucción recibida, el dispositivo de protección analiza si el resultado de la ejecución debe ser almacenado en la memoria de la computadora o en la memoria del dispositivo de protección y lo almacena de ser así.

19. Método de protección de programas de computación, contra la copia y el uso no autorizado, según la reivindicación 18, caracterizado porque en dicha etapa (e) de Ejecución de módulos, luego de dicha ejecución de la instrucción, el dispositivo de protección vuelve a obtener código máquina del módulo que está siendo ejecutado y continúa la ejecución dentro del dispositivo de protección hasta la finalización del módulo.

20. Método de protección de programas de computación, según la reivindicación 18, caracterizado porque en dicha etapa (e) de Ejecución de módulos, luego de dicha ejecución de la instrucción, el dispositivo de protección vuelve a obtener código máquina del módulo que está siendo ejecutado y continúa la ejecución dentro del dispositivo de protección hasta la presencia de una instrucción que interrumpa y direccione la ejecución del programa a la computadora.

21. Método de protección de programas de computación, contra la copia y el uso no autorizado, según la reivindicación 20, caracterizado porque

en dicha etapa (f) de retorno a la computadora, el dispositivo de protección retorna el hilo de ejecución a la computadora enviándole a la misma la actualización de todos los registros de su procesador.

22. Equipo para realizar el método de protección de programas de computación, contra la copia y el uso no autorizado, según cualquiera de las reivindicaciones anteriores, caracterizado porque está integrado por una computadora donde se procesa la parte pública del programa de computación protegido, un dispositivo de protección (donde están almacenados los "módulos" que componen la parte privada del programa de computación protegido), un medio de comunicación entre la computadora y el dispositivo de protección, un programa adicional que auspicia de interfaz de comunicación y recursos de la computadora, estando estos recursos compartidos con el dispositivo de protección durante la ejecución de dichos módulos dentro de dicho dispositivo.

23. Equipo para realizar el método de protección de programas de computación, según las reivindicaciones 22, caracterizado porque dicho dispositivo de protección consta como mínimo de un microprocesador, memoria volátil y memoria no volátil donde se almacenan los módulos obtenidos, y donde dicha memoria no puede ser leída desde el exterior.

24. Equipo para realizar el método de protección de programas de computación, según la reivindicación 23, caracterizado porque dicho medio de comunicación entre la computadora y el dispositivo de protección, es uno de los puertos de comunicación que posee la computadora.

25. Método de protección de programas, contra la copia y el uso no autorizado, según cualquiera de las reivindicaciones 1 a 21, caracterizado porque es usado para proteger sistemas de control de

procesos.

26. Método de protección de programas, contra la copia y el uso no autorizado, según cualquiera de las reivindicaciones 1 a 21, caracterizado porque es usado para proteger sistemas de control de equipos.

27. Método de protección de programas, contra la copia y el uso no autorizado, según cualquiera de las reivindicaciones 1 a 21, caracterizado porque es usado para proteger programas para computadoras portátiles.

28. Método de protección de programas, contra la copia y el uso no autorizado, según cualquiera de las reivindicaciones 1 a 21, caracterizado porque es usado para proteger programas para equipos embebidos.

29. Método de protección de programas, contra la copia y el uso no autorizado, según cualquiera de las reivindicaciones 1 a 21, caracterizado porque es usado para proteger programas de computación.

30. Método de protección de programas, contra la copia y el uso no autorizado, según cualquiera de las reivindicaciones 1 a 21, caracterizado porque el programa de computación protegido contiene múltiples hilos de ejecución (conocidos como "multi-thread")

31. Método de protección de programas, contra la copia y el uso no autorizado, según cualquiera de las reivindicaciones 1 a 21, caracterizado porque es usado para proteger programas de computación utilizados en red bajo el régimen de "licencias", donde se limita la cantidad de programas de computación protegidos que se pueden ejecutar al mismo tiempo.

32. Método de protección de programas, contra la copia y el uso no autorizado, según cualquiera de las reivindicaciones 1 a 21 , caracterizado porque es usado para proteger programas para telefonía celular.

Jorge Aníbal FERNÁNDEZ

BELLONI, Fabián

SCHIAVONI, Juan

SCOCHET, Gabriel

SEMINO, Darío

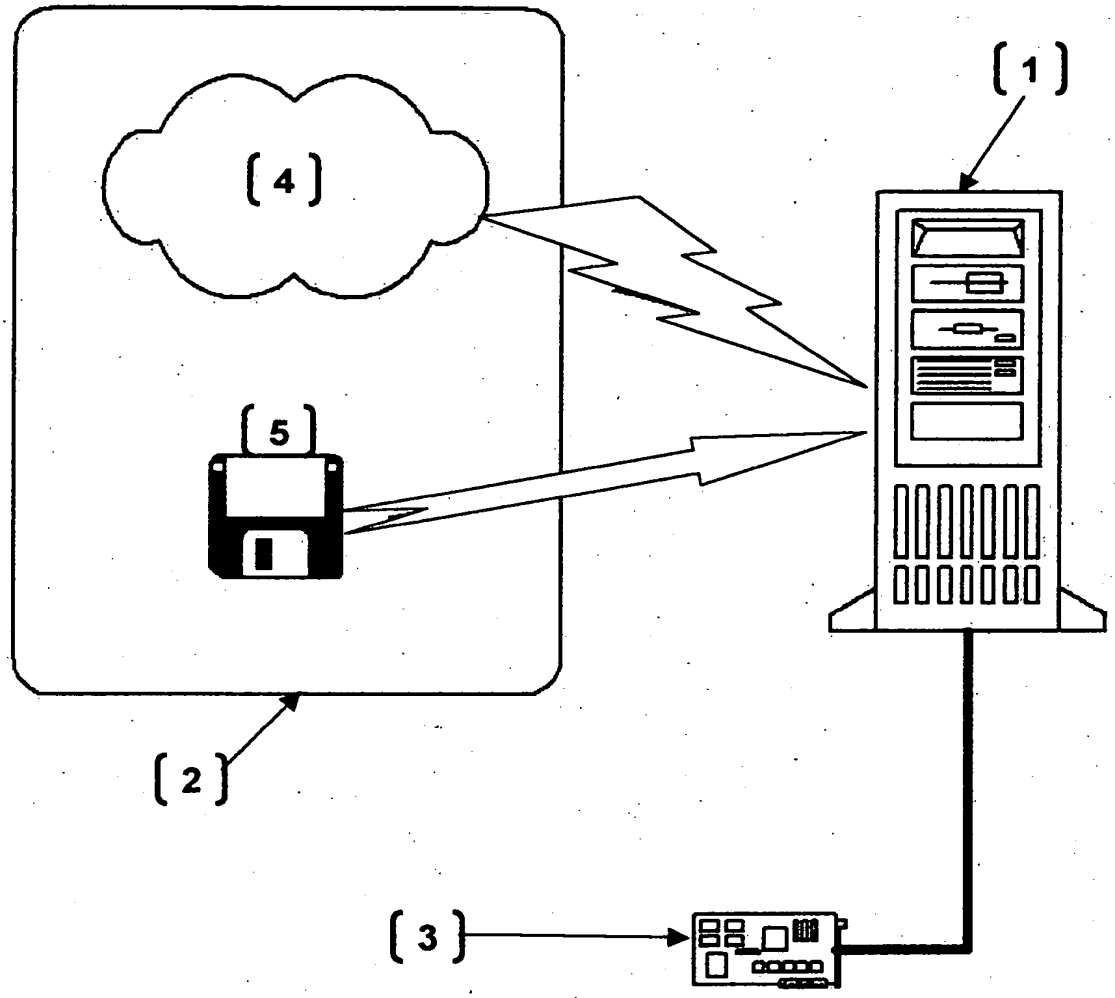


Figura 1

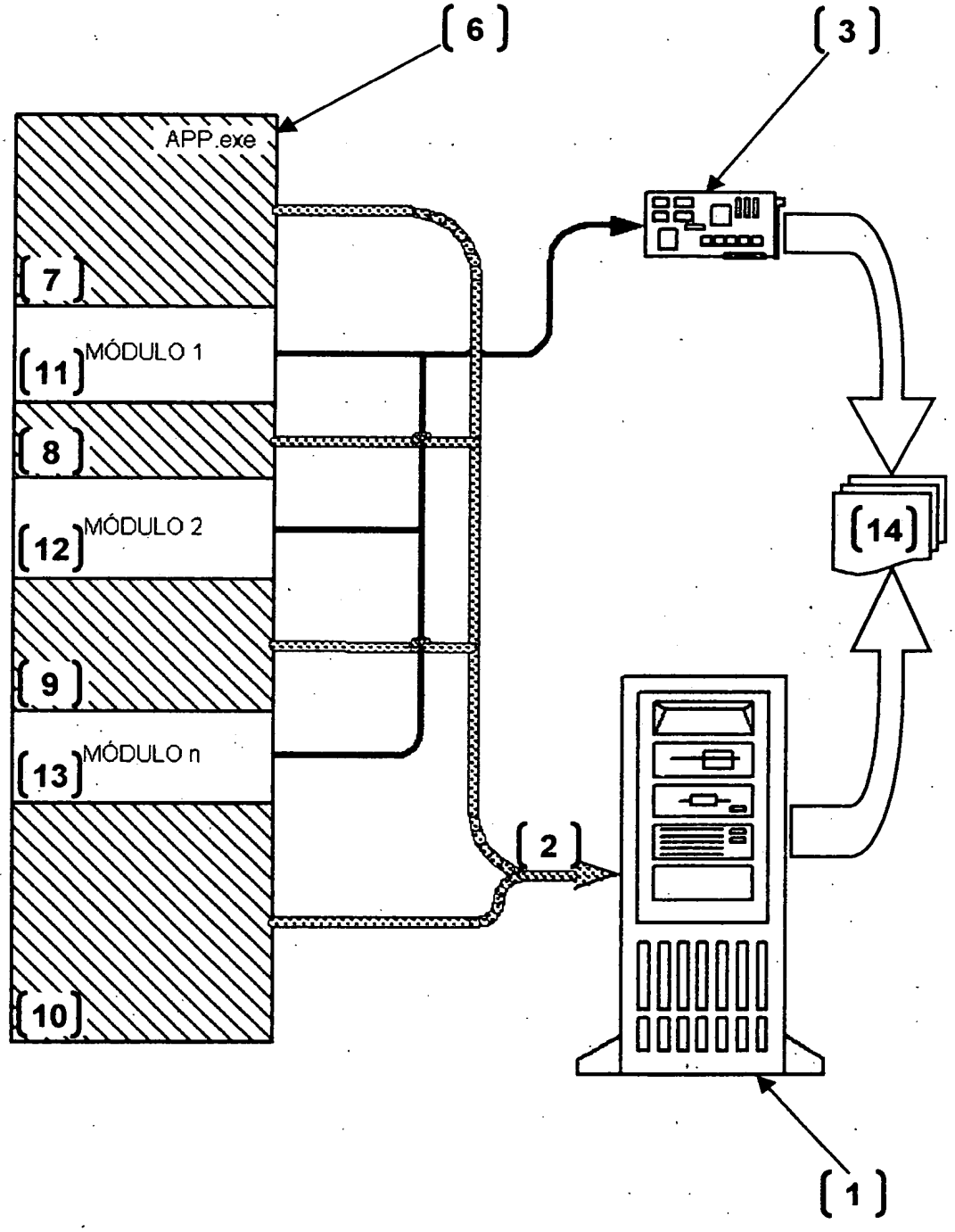


Figura 2

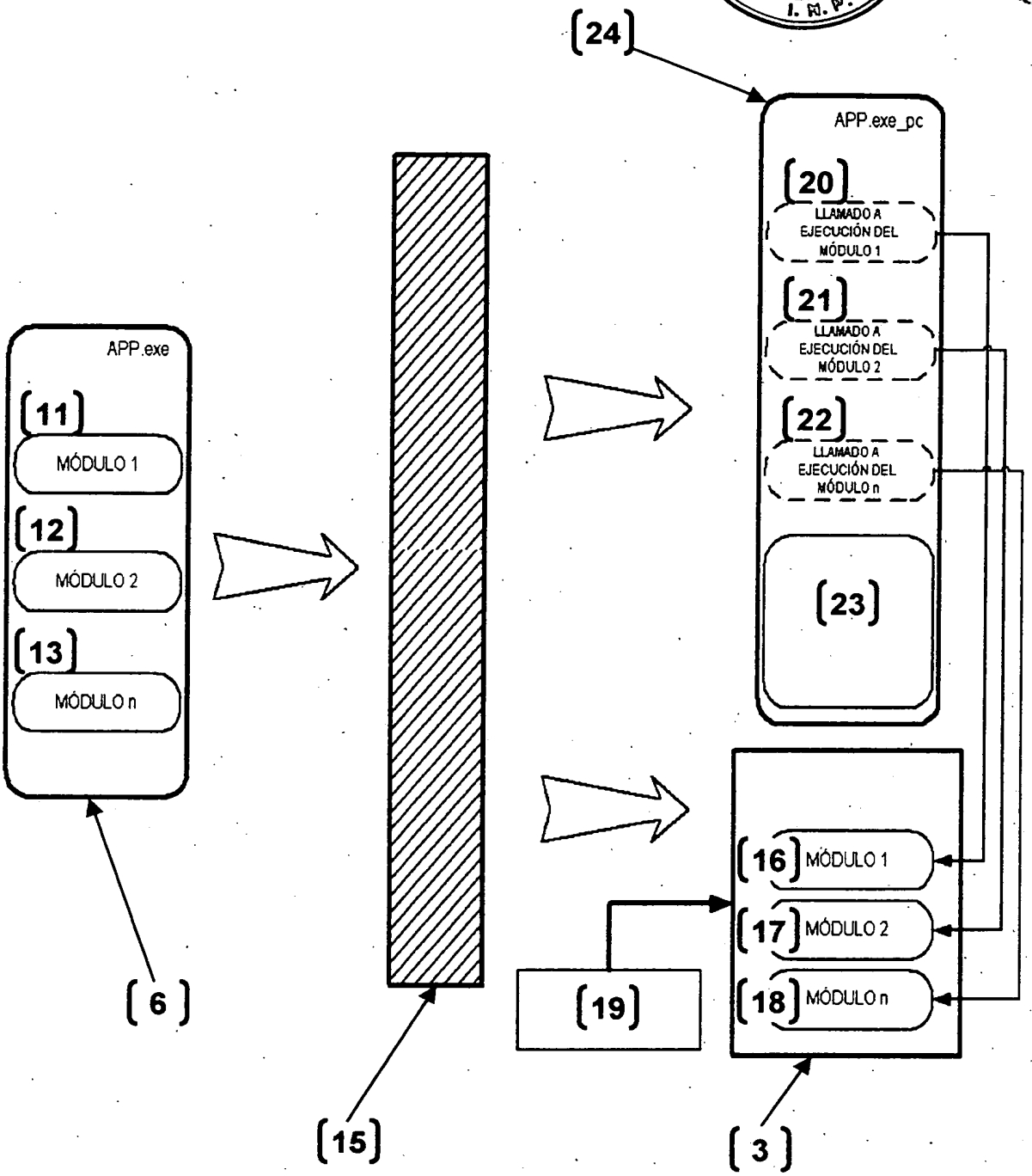


Figura 3

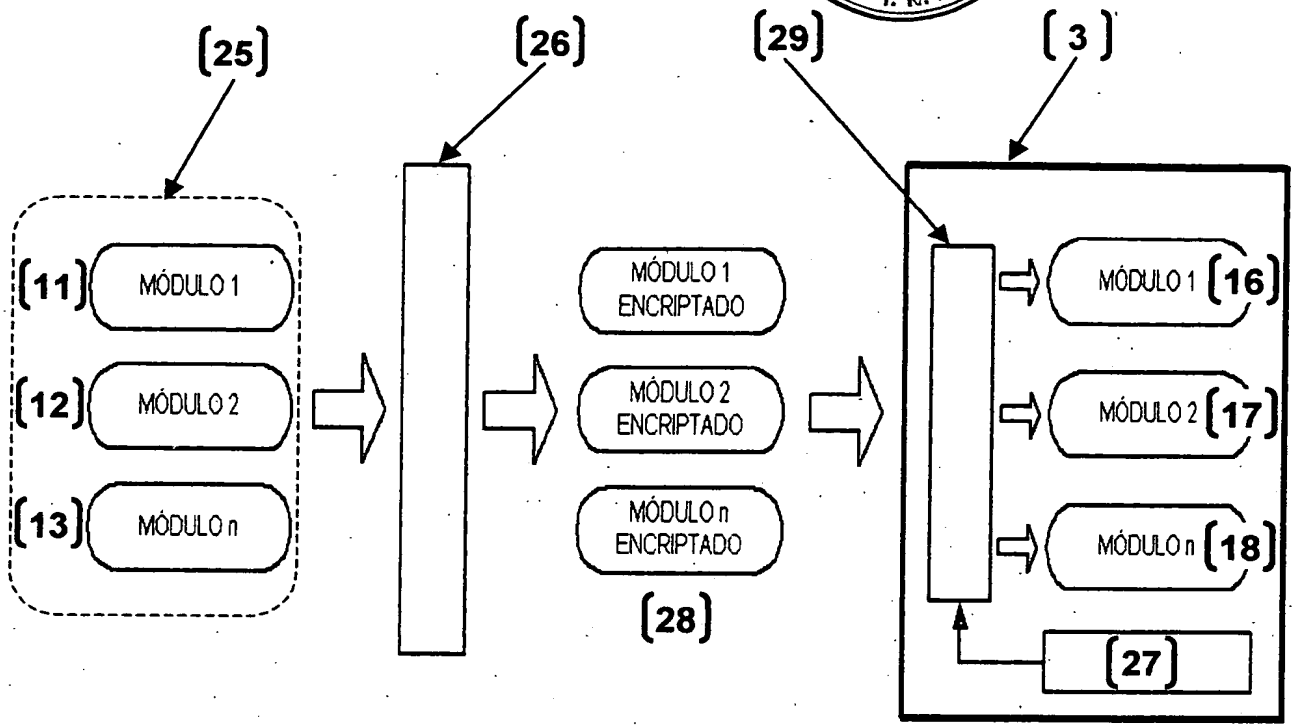


Figura 3b

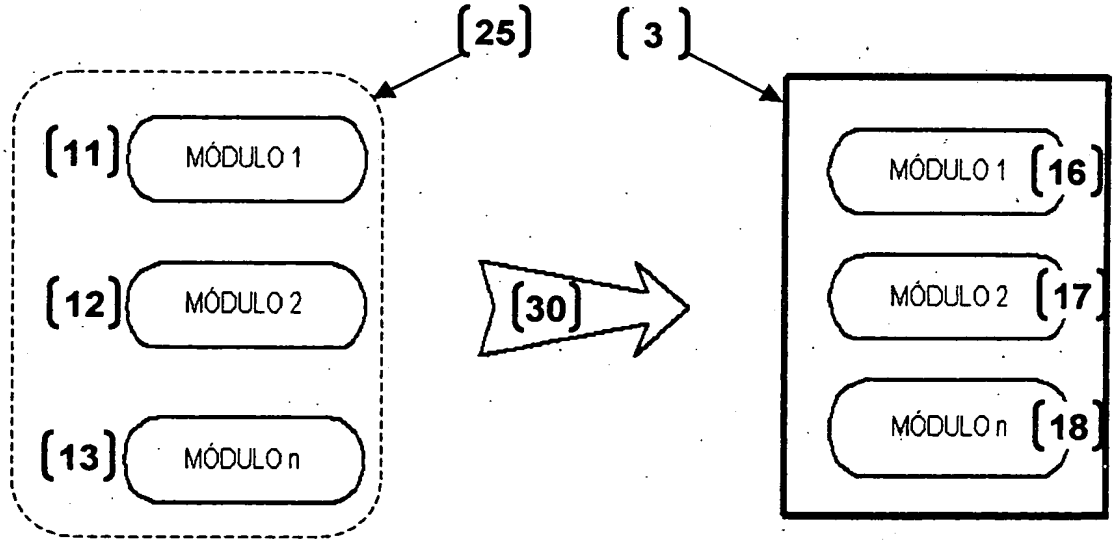


Figura 3c

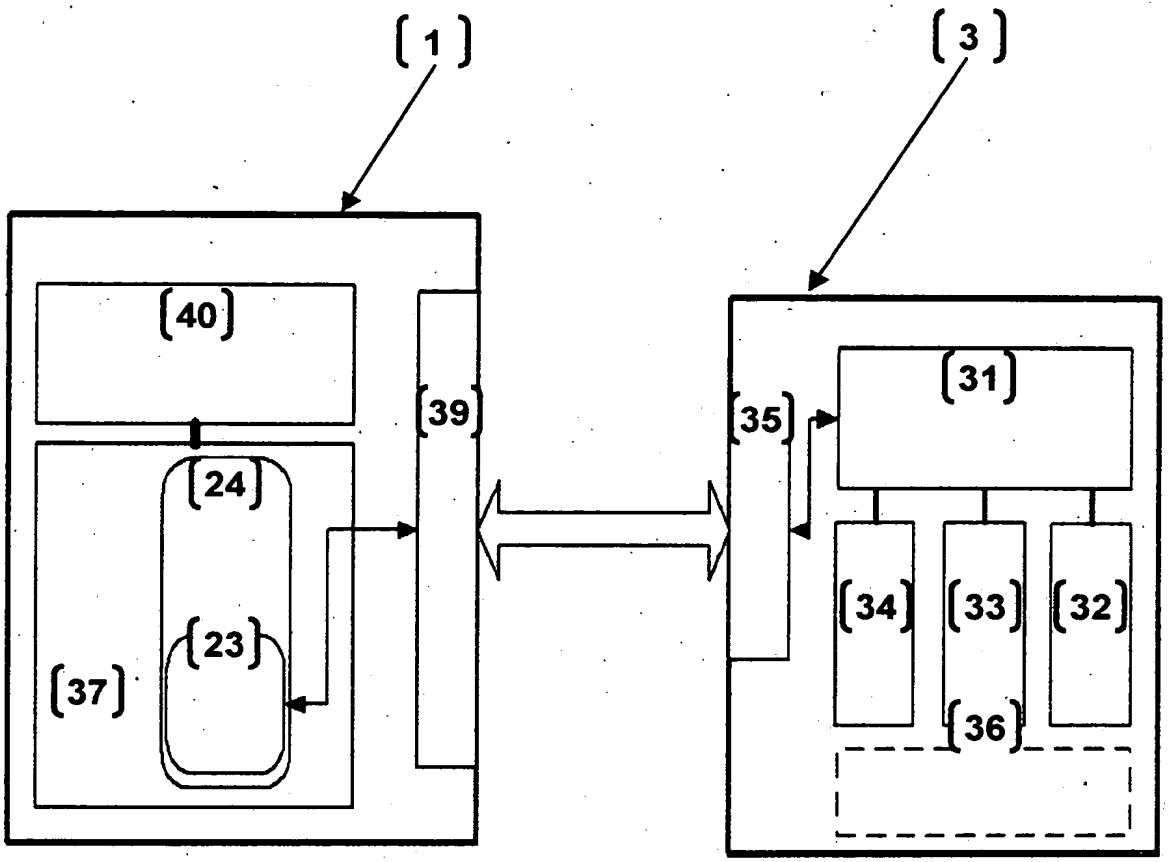


Figura 4

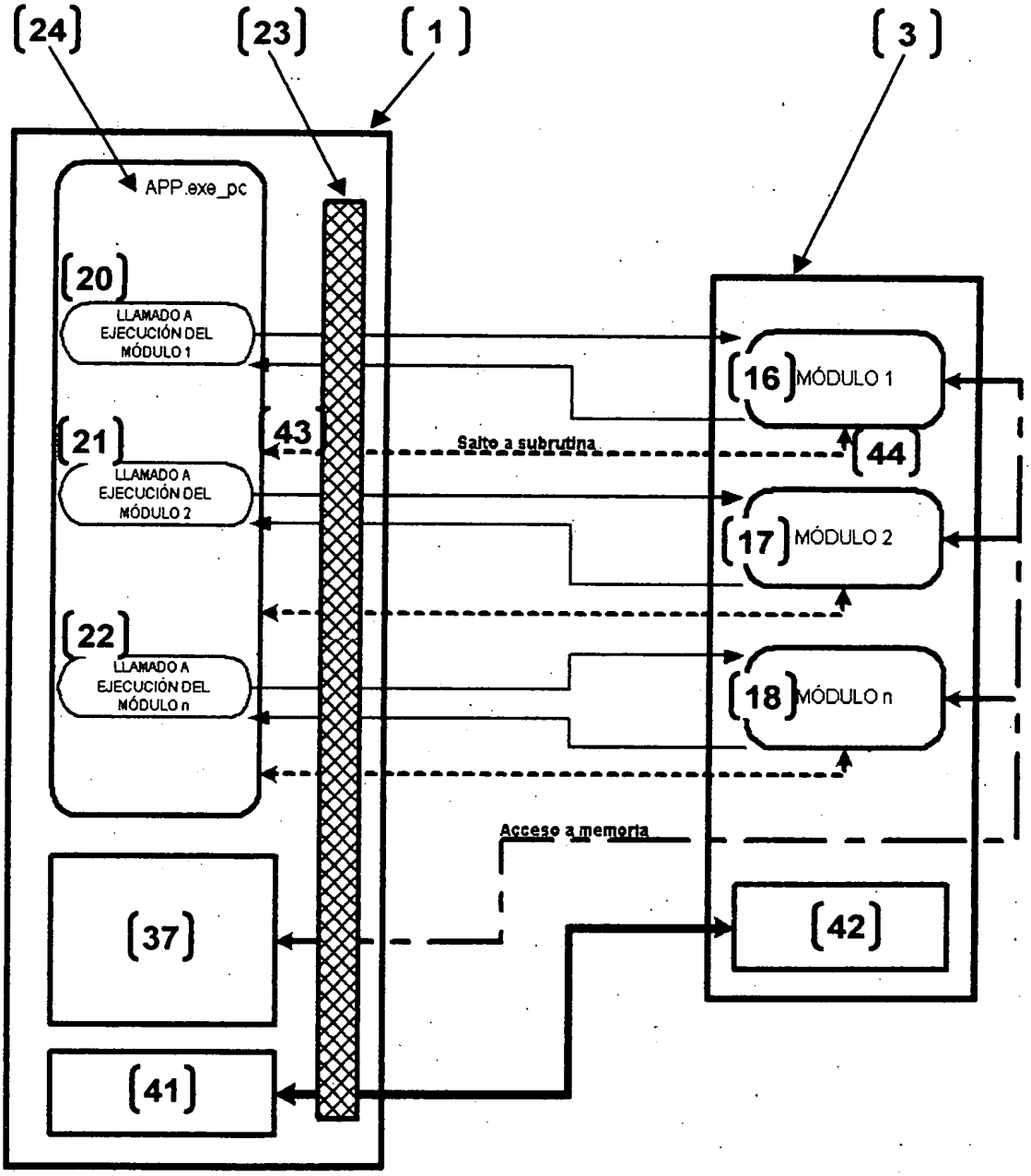


Figura 5

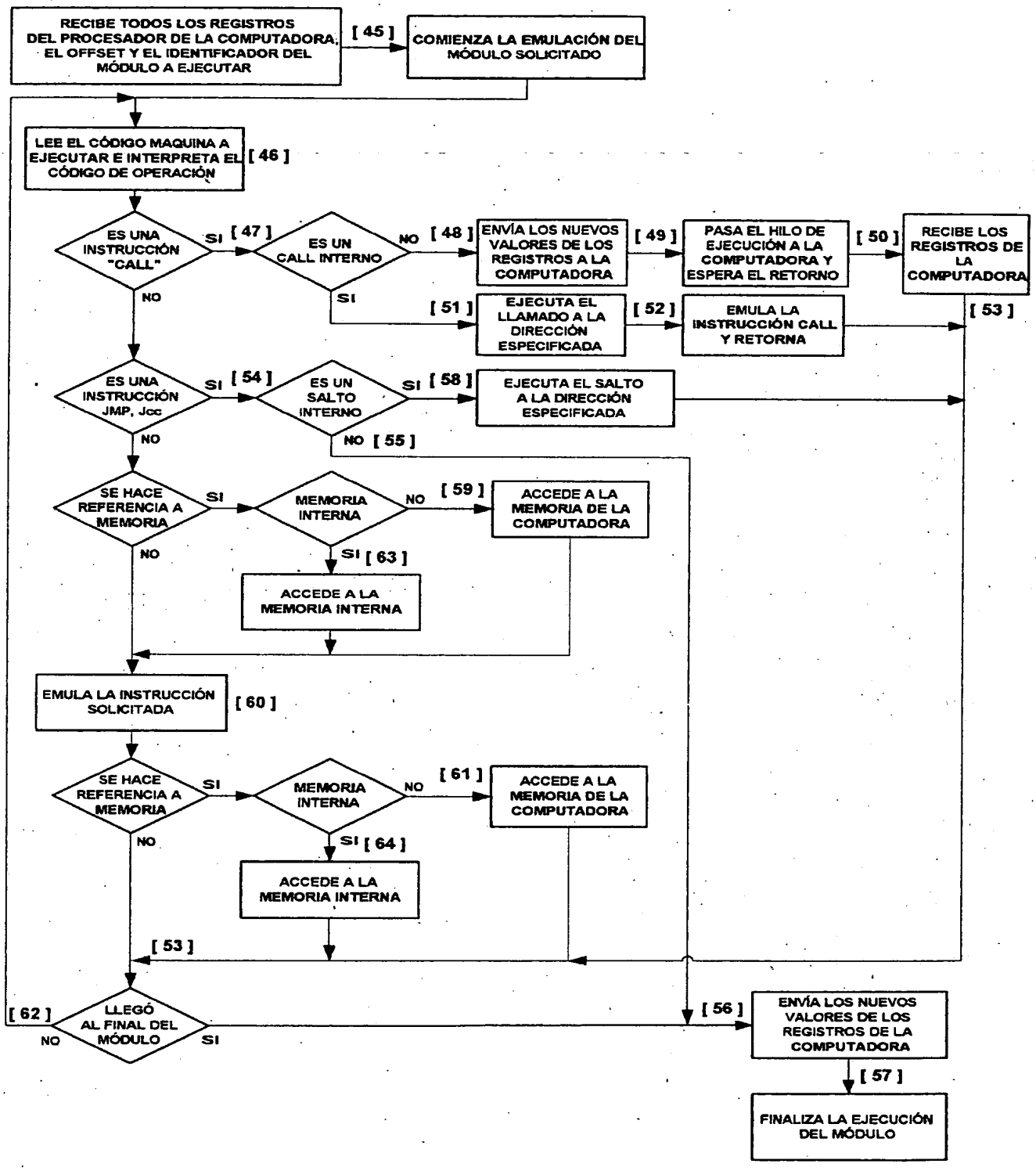
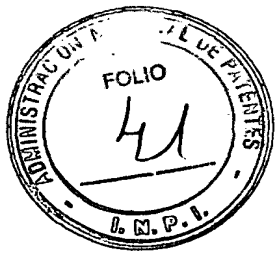


Figura 6



RESUMEN

La presente invención se refiere a un método de protección de programas de computación, contra la copia y el uso no autorizado, que se realiza mediante la ejecución de partes seleccionadas del código máquina del programa a proteger (protegido), o "módulos", que son extraídos y almacenados dentro de un ambiente seguro conformado por un "dispositivo de protección". Dichos módulos son reemplazados en el programa de computación protegido por llamados a ejecución de dichos módulos dentro del dispositivo de protección, donde durante esa ejecución la "computadora" (que ejecuta el programa protegido) comparte sus recursos con dicho "dispositivo de protección", de tal manera que pueden ser utilizados por éste último.

Otro aspecto de la invención es el equipo necesario para realizar dicho método.

La invención puede ser aplicada para proteger sistemas de control de procesos, sistemas de control de equipos, programas para telefonía celular, programas para computadoras portátiles, programas para equipos embebidos, programas de computación en general y controladores en general.